RISK MANAGEMENT/COMPLIANCE

The OKI Group is working to reinforce risk management under the Risk Management Committee. In accordance with our "Compliance Commitment" and, in order to perform corporate activities fairly, we are focusing on the enhancement of training, and we have established consultation and reporting contacts.

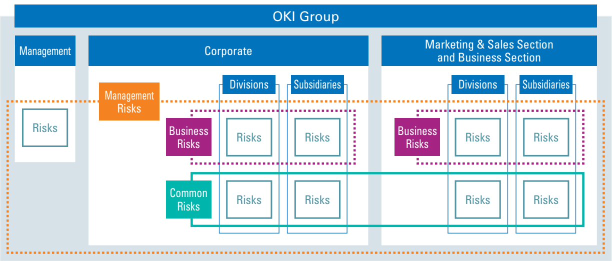
●Risk Management Initiatives

OKI has established the Risk Management Committee, chaired by the President, to ensure that risks related to the OKI Group's corporate activities are grasped and managed properly. The Committee deliberates and decides on basic policies for risk management and identifies risks to be managed based on such policies and the division responsible for said risks. It also deliberates and decides on policies for preventing the materialization of risk and policies to address crisis scenarios.

Risks to be managed are defined and classified into three categories: "management risks" that should be considered at the management level, "business risks" that should be recognized and identified in relation to business activities, and "common risks" that are common to each company and division and should be managed across the Group. Of these risks, the responsible control division deploys preventive measures for common risks within the Group, while the Compliance Committee (see next section) regularly checks the implementation status. In this way, we are putting in place a sound risk management cycle. In fiscal year 2020, OKI identified the business risks for each of its business groups in order to strengthen the management of these risks. OKI is making progress in creating the management cycle and developing its framework.

To swiftly identify and resolve problems, we also established the OKI Group Risk Incidents Reporting System, which ensures that potential risk events, crises, and situations that may lead to such events are promptly reported to the Risk Management Committee.

Risks to Be Managed



Management risks are risks that should be managed at the management level.

Related information: Website "Business and Other Risks"
https://www.oki.com/en/ir/corporate/risk.html

●Initiatives to Promote Compliance

The OKI Group has established the Compliance Committee (with the Chief Compliance Officer as Committee Chairman) in accordance with the top management's Compliance Commitment thereby striving to ensure rigorous compliance. The Committee regularly monitors the management progress of the common risks identified by the Risk Management Committee. The Committee also deliberates and decides on compliance training plans and oversees their implementation. Moreover, we implement fixed-point observations on conduct and awareness relating to compliance of executives and employees, and to make the most of such measures, we implement compliance awareness surveys on an ongoing basis.

In order to discover and rectify improper activities at an early stage, we have established whistle-blowing system (in-house contact point, Group-wide contact point, and external contact point) to enable anonymous reports, as well as reports to outside directors and Audit & Supervisory Board members at every Group company, and stipulated whistle-blowing regulations such as those about the protection of whistle-blowers. In fiscal year 2020, 41 reports and consultations were received at the OKI Group in Japan.

●Ongoing Compliance Training

The OKI Group has appointed compliance managers and promoters (around 350 in total) who play a key role promoting compliance in the workplace at each company and division in Japan. We also hold regular training sessions for these compliance managers and promoters. We are holding ongoing anti-monopoly law training centered on the marketing & sales section. In fiscal year 2020, the group training was held via video conference in order to prevent the spread of COVID-19.

We provide e-learning to all Group employees in Japan on topics related to shared risks, such as personal information protection, information security, and common risks. We also have tools in place to ensure that the content of the training is widely disseminated. These include regular reports of case studies on compliance issued via our intranet and internal newsletters.

In fiscal year 2018, we started a unified e-learning compliance training program for some overseas Group companies, and we added a subsidiary in Vietnam to the program in fiscal year 2020.

Main Compliance Training Programs (for the OKI Group in Japan) in FY2020

Training Overview	Subject Employees	Attendance Rate
Compliance manager training September–December 2020 (video) Theme: Introduction of OKI group risk management system, contracting/sub-contracting, client asset management, and risk management at workplace	Domestic Group managers/promoters	100% (approx. 350 persons)
Anti-monopoly Act training December 2020 to March 2021 (video)	Domestic Group employees of related divisions (sales, etc.)	100% (approx. 2,500 persons)
Personal information protection and information security e-learning (regular and start anytime sessions) Regular session (simultaneous training) held August to September 2020	All domestic Group employees	Simultaneous training: 99.9%
Workplace compliance e-learning (regular and start anytime sessions) Regular session (simultaneous training) held December 2020 to January 2021	All domestic Group employees	Simultaneous training: 100%

●Approaches to Anti-Corruption

The OKI Group is promoting initiatives to prevent corruption, which is a global issue, based on the "OKI Group Anti-Corruption and Anti-Bribery Policy" that we established in fiscal year 2013.

The "OKI Group Anti-Corruption and Anti-Bribery Policy" complies with anti-corruption laws and regulations that apply in each country and region where the OKI Group operates, such as the Japanese Unfair Competition Prevention Act, the US Foreign Corrupt Practices Act, and the UK Bribery Act. The policy defines the basic requirements for complying with laws and regulations and conducting business appropriately. As company bylaws, we established specific rules for recording the exchange of the gifts and receiving/offering entertainment, and compliance with these rules at each Group company is monitored annually by OKI's responsible division.

In fiscal year 2020, there were no issues related to bribery or corruption in the OKI Group.

●Emergency and Disaster Response

The OKI Group has established Safety Countermeasure Committees at its domestic and overseas sites, as well as at subsidiaries, in order to ensure "protect people's lives," "prevent secondary accidents," "contribute to local communities and foster good relationships with them," and "continuity of business operations" in the event of disasters. Among them, OKI established and conducts regular reviews of the Business Continuity Management (BCM) / Business Continuity Plan (BCP) based on the BCM Development Guidelines in each division for the "continuity of business operations."

In fiscal year 2020, the COVID-19 Task Force that was established in January 2020 conducted initiatives to prevent the spread of the virus and maintain business continuity, such as transmitting information about the status of the virus in Japan as well as identifying and handling those infected inside the Group. OKI is also striving to respond quickly and appropriately by continuously reviewing initial countermeasures for natural disasters, such as earthquakes, typhoons, and floods.

INFORMATION SECURITY

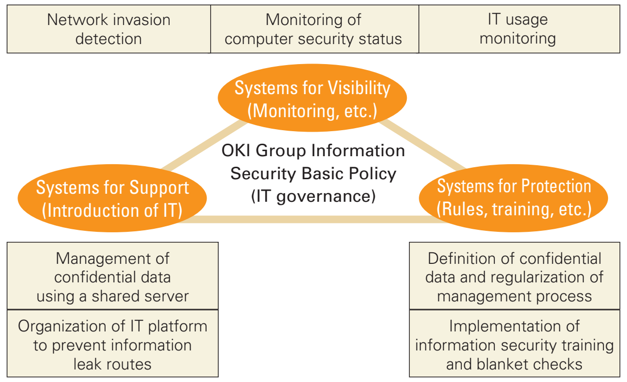
Based on the OKI Group Information Security Basic Policy, the OKI Group has established a system to ensure information security to properly manage and protect company and customer information.

●Policy on Information Security Initiatives

The OKI Group is building a robust IT infrastructure to support its business growth. As part of this effort, we are working to strengthen information security from the perspective of minimizing management risks. As our Risk Management Committee has defined "electronic information leakage" and "cyber attack" as common risks, we have made it clear that measures for information security are an important part of management and we are proceeding with them.

We are also promoting a wide range of measures based on the three mechanisms shown in the figure below. In addition, we established OKI-CSIRT* as a specialized security incident response organization tasked with strengthening our ability to prevent and respond to incidents.

*CSIRT: Computer Security Incident Response Team


Network invasion detection
Monitoring of computer security status
IT usage monitoring
Systems for Visibility (Monitoring, etc.)
OKI Group Information Security Basic Policy (IT governance)
Systems for Support (Introduction of IT)
Systems for Protection (Rules, training, etc.)
Management of confidential data using a shared server
Organization of IT platform to prevent information leak routes
Definition of confidential data and regularization of management process
Implementation of information security training and blanket checks

●Strengthening Information Security Measures

The OKI Group constantly monitors global trends and promotes information security measures in Japan and overseas. We also establish information security guidelines in each country and region, appoint security managers at each site, and introduce various risk management tools.

In fiscal year 2020, all divisions of OKI in Japan, excluding certain parts of the Corporate Group, as well as three subsidiaries newly acquired ISMS certification. In this way, OKI aims to strengthen information security system. In order to further strengthen IT governance overseas, OKI is proceeding with establishing communications systems and rules, deploying countermeasure tools, and aligning the monitoring environment. In fiscal year 2020, OKI deployed various tools, including EDR*.

●Enhancing Protection of Personal Information

We in the OKI Group have enhanced protection of personal information, based on the Privacy Policy. We have committed to the protection of personal information under the leadership of our Chief Privacy Officer. Privacy managers have been appointed in all divisions and subsidiaries. OKI is taking measures based on regulations for the personal information protection laws in the EU, Brazil, and Thailand (EU: GDPR, Brazil: LGPD, Thailand: PDPA), where Group companies are located.

As of June 2021, seven companies of the OKI Group have received PrivacyMark certification in Japan.

*EDR (Endpoint Detection and Response): Technology that constantly monitors and responds to threats at endpoints of computer systems